A Study of Congestion Control and Reliability Mechanism in Opportunistic Mobile Ad Hoc Networks

T.C.Ezhil Selvan[1], Assistant Professor
Sri Ramakrishna Institute of Technology, Coimbatore
Dr.P.Malathi[2], Principal
Bharathiyar Institute of Engineering for Women, Salem.
S.Ezhilin Freeda[3], Assistant Professor
Sri Ramakrishna Engineering College, Coimbatore
ezhilselvan85@gmail.com, pmalathi2004@yahoo.co.in & ezhilinfreeda@gmail.com

Abstract—Opportunistic networks are a type of Mobile Ad hoc Networks (MANETs) where links between mobile nodes arise unpredictably and where a whole end-to-end path between source and destination infrequently happens at one time. Two important functions, conventionally provided by the transport layer, are certifying the reliability of data transmission between source and destination, and certifying that the network does not become congested with traffic. However, modified versions of TCP that have been offered these functions in MANETs are ineffective in opportunistic networks. In addition, opportunistic networks require dissimilar approaches to those adopted in the more common irregularly connected networks. In this paper we identify the state of the art of proposals for transfer reliability and storage congestion control schemes in opportunistic networks. We discuss possible mechanisms for transfer reliability service, i.e. hop-by-hop protection transfer and end-to-end return acceptance. We also identify the requirements for storage congestion control and categorize these issues based on the number of message reproductions distributed in the networks. For single-copy forwarding, storage congestion management and avoidance mechanism are argued. For multiple-copy forwarding, the core congestion control mechanisms were the replication managing and drop policy.

Keywords: MANETs, recurrently connected networks, opportunistic networks, reliability, storage congestion control.

1. INTRODUCTION

Mobile adhoc networks (MANET) are infrastructure less networks where nodes can move frequently. One node can directly transfer with another if they are within radio communication range. A node can simultaneously work both as a source or endpoint of a message and as convey for other messages. A message crosses the network by being transmitted from one node to another node until it reaches its destination. Since the nodes are moving, the network topology regularly changes and so finding a delivery path to a destination is a challenging task. Building end to- end delivery paths and ensuring robust message delivery in the face of dynamic topology changes are tasks that have been addressed in MANETs, and an plenty of routing and transport protocols have been proposed. In all these protocols, it is indirectly assumed that the network is endlessly connected and that there exists at end-to-end route between all source and destination pairs in the networks.

However, in some situations complete end-to-end paths infrequently or not ever occur between sources and destinations within the MANET, due to high mobility of node or low node density. These networks may experience frequent partitioning, with the disconnections for long-lasting periods. As significance, the end-to-end transfer delays in these *irregularly*

connected networks (ICN) are much larger than typical IP data transfer delays in conventional networks such as the Internet. In the literature, irregularly-connected networks are often referred to as *delay-* or *disruption tolerant networks* (DTN); its related with the Delay / Disruption Tolerant Networking architecture.

Although research in Irregularly Connected Networks routing is now well established, research in Irregularly Connected Networks transfer reliability and congestion control is still in its early stages. So far, most of the work in these areas has been battered at applications in deep space communications, for example the Internet. Within Irregularly Connected Networks we can classify opportunistic networks, which are networks where contacts between mobile nodes arise randomly because the node's movement is effectively random, and where the duration of each node contact is also random. The experiments of developing effectual algorithms for opportunistic networks are different from those of typical Irregularly Connected Networks such as deep space networks.

2. IRREGULARLY CONNECTED NETWORKS

Irregularly Connected Networks happens in challenged network environments; examples include high space communications where links take high delays [2][3], sparse sensor networks wherever connectivity is repeatedly irregular [4], wildlife watching networks where wildlife motions are unpredictable and in human (social) networks where connectivity occurs opportunistically, e.g. pocket-switched networks [6]. ICNs does not fulfill old networking expectations, where end-to-end paths always exist, and the networks have low propagation delays, low bit error rates, and high bandwidth. As a result, communication protocols built for these old networks, e.g. the Internet and MANETs, are not able to consider data communication efficiently in Irregularly Connected Networks. End-to-end communication using the TCP/IP protocol suite is ineffective against the impairments of Irregularly Connected Networks.

In the network layer, MANET routing protocols, such as OLSR [7], AODV [8] and DSR [9], will drop packets if the destination cannot be found. In the transport layer, TCP variants for MANETs, such as TCP-EFLN [10], A-TCP [11], TCP Snoop [11] and TCP-BuS [11], will also break down in ICNs: these protocols think that the network is continuously connected, and they consider link troubles, due to node movement or link layer conflict, as temporary and short-term events. TCP eventually fails in Irregularly Connected Networks, since link disconnections occur frequently and the round trip delays are too long. Hence, modified protocols needed to be develop for Irregularly Connected Networks.

a) Delay-Tolerant Networking (DTN) Architecture

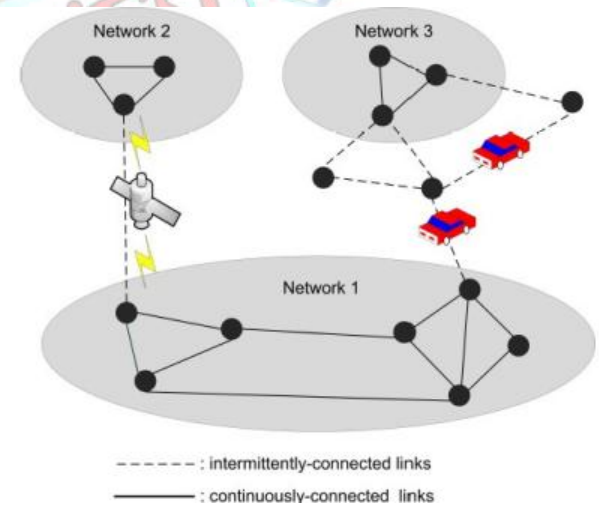

Fig 1. Irregularly Connected Network (ICN)

An example Irregularly Connected Networks scenario is illustrated in Fig. 1, where three networks, each of which is continuously connected, are linked by irregular connections, namely a satellite link (between

networks one and two) and a vehicular network (between networks one and three). The satellite link is scheduled and predictable, whereas the vehicle-based links are irregular and therefore adaptable. The vehicle contacts, when they arise, might be of long or short duration. Irregularly Connected Networks nodes (or simply "nodes" in this paper) are responsible for managing data transfer between the temporarily disconnected networks. As nodes come into contact, they can transfer data, for example sending and receiving bundles.

A bundle is an arbitrary sized data unit and has a time-to-live before bundle expiration; in the literature as well as in this article the term "message" is also used to refer to a "bundle". When a peer node or a link or path is currently not available, a node waits, storing the bundle or forwarding it to another node that may have better a chance of delivering the bundle to its destination. Communications between disconnected areas can be performed by a *store and forward* (SF) mechanism, as in the satellite communications between network one and two or a *store carry forward* (SCF) mechanism, e.g. in the vehicular network between network one and three. In SF, when there is no next hop known or no available link to the known next hop, bundles are stored in a node buffer waiting for the next contact event. In SCF, physical message carriers, such as vehicles, humans or message ferries, are added to carry and forward messages between disconnected areas.

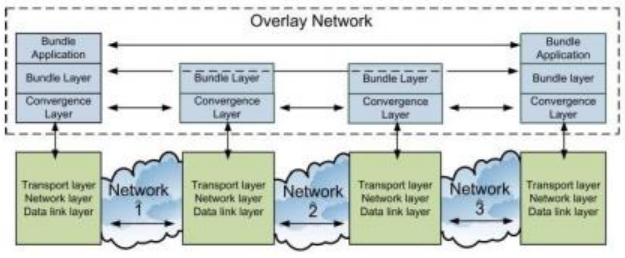

Fig 2. DTN Architecture

For these mechanisms, the probability of node contact, the node contact period and node resource size (e.g. storage and energy) are key attributes for effective data delivery in Irregularly Connected Networks.

The architecture for delay and disruption tolerant networking (DTN) (Fig. 2) was developed by the Internet Research Task Force (IRTF) DTN Research Group (DTNRG) [10]. This architecture considers irregularly-connected networks that suffer from recurrent partitions and which may consist of more than one protocol family. The basis of the DTN architecture lies in the Internet, which addresses the main issues of high space communications, i.e. long delays and high packet losses.

However, more generally this architecture can be utilized in various operational environments that are subject to disturbance and discontinuation. As depicted in Fig. 2, DTNRG defines three layers for DTN communications that stand on upper of network-specific layers known as the TCP/IP protocol stack, with these three layers forming an overlay network.

The layers are the build application layer, bundle layer and convergence layer. An application uses DTN nodes to send and receive Application Data Units by means of the bundle application layer. A bundle application protocol maintains point-to-point communication between the applications in the source and destination nodes.

The convergence layer provides a direct mapping between the build layer and lower protocol layers, such as the transport layer (e.g. TCP or UDP) or link layer [10]). Finally, at the heart of the DTN architecture the package layer manages *hop-by-hop* message transfers from source to destination when link disruptions or high delays occur. The DTN architecture defines important data delivery tasks at the bundle layer, such as routing and forwarding, reliability and care transfer, congestion and flow control and security [11].

b) ICN Routing Strategies

Routing in Irregularly Connected Networks is more complicated than in MANETs due to the lack of up-to-date network topology information. Here we briefly review Irregularly Connected Networks routing strategies since, as we shall see, the routing algorithms disturb design choices about transfer and congestion control mechanisms. Irregularly Connected Networks routing protocols typically use historical node contact data to predict future network topology. Three categories of regularity of node contacts can be defined, specifically *on-demand contact*, *scheduled or predicted contact* and *opportunistic contact*.

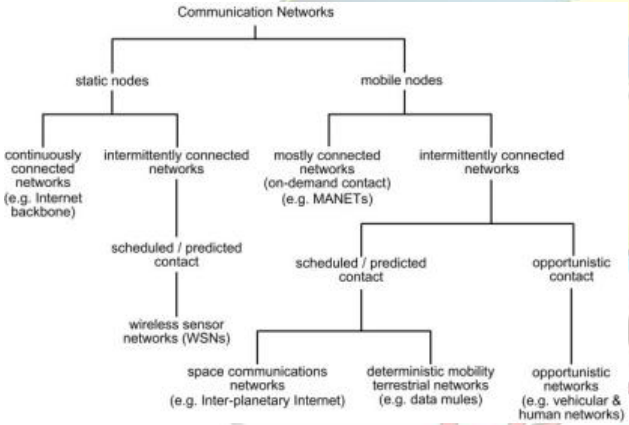

Fig 3. Classification of Communication Networks

In Fig. 3, we use these categories in a taxonomy of communication networks. We first split the networks, based on node mobility, into static and dynamic nodes. Static node networks can be either continuously connected (such as the Internet backbone) or intermittently connected. The latter division includes Wireless Sensor Networks (WSNs), whose nodes preserve energy by disabling their radio connection when not required. In the mobile node branch of the classification, we again distinguish between networks where links between nodes generally exist and networks where node contact is recurrent. In MANETs, links are assumed to be always or usually available when needed; this is also recognized as *on-demand contact*. We use the regularity of node contact to further divide the intermittently connected mobile networks: we differentiate between networks where node contacts are predicted (e.g. the Interplanetary Internet) or scheduled (for example, data mules [9]), and networks where node contacts are not generally predictable, such as vehicular networks and normal networks. It is this concluding category that is commonly called *opportunistic networks*.

In scheduled or unscheduled contact, future node contacts are known in advance. Two examples of this are a link between an earth position and a satellite where the satellite's view schedule is known in advance, and a link between wireless sensor devices and a data mule, which visits a sensor device at regular times to collect data. In these cases, message transmissions can be scheduled in advance so that optimal delivery performance can be achieved. Deterministic routing protocols, such as Space Time Routing [7], Tree Approach [8] and Modified Shortest Path [19], are able to achieve a high delivery ratio while minimizing consumption of node resources, for occasion by applying a *single-copy* forwarding strategy. In this strategy, at any instant only one copy of a message is circulating in the network.

In opportunistic meetings, a node knows nothing about future contacts or network topology. In this case a routing strategy can stochastically estimate future node contacts; it can also forward several copies to different nodes to increase delivery probabilit. For example, in widespread routing [10], a node floods duplicates of a message to all its neighbors within transmission range so that the copies are quickly distributed throughout the network. As this oblivious forwarding assumes limitless node resources, it tends to deplete

node resources rapidly which in turn significantly degrades the network performance. Alternatively, a routing strategy may use contact history or mobility patterns to calculate the probability of a node being talented to deliver a message to the end side. A copy of the message is only forwarded to those nodes that satisfy given routing criteria.

A contact history based routing algorithm such as Prescient [2] approximations a delivery predictability based on the previous contact times for each known destination, and estimates the ability of a node to deliver a message to its destination. As a 3rd approach, a social-based routing algorithm, such as SimBet [5] or Bubble Rap [4], uses principles derived from the structure of social networks, and forwards duplicates of a message to nodes that have a greater capacity of contact (a larger popularity or *centrality*) than the current node. For a more detailed discussion of Irregularly Connected Networks routing protocols, readers are referred to [5][6] and the references therein.

3.CONGESTION CONTROL AND RELIABILITY IN OPPORTUNISTIC MOBILE ADHOC NETWORKS

Opportunistic networks must have certain features that are distinct from Irregularly Connected Networks in general and high space networks in specific. In opportunistic networks, nodes usually move at random and link disruptions due to node mobility are stochastic. In addition, the long transfer delay is due to the unpredictability of contact events and the limited contact period when nodes are within possible location, rather than being caused by long propagation delays. The authors in 33 argue that a node can exploit its mobility to really carry messages between disconnected parts of the network to attain ultimate delivery and to increase complete network volume. We therefore see that in SCF networks the challenges and requirements in scheming transfer reliability and congestion control vary from those in store-forward (SF) networks, such as deep space networks.

We currently define a basic opportunistic network scenario and display how the transfer reliability and congestion control functions might cooperate.

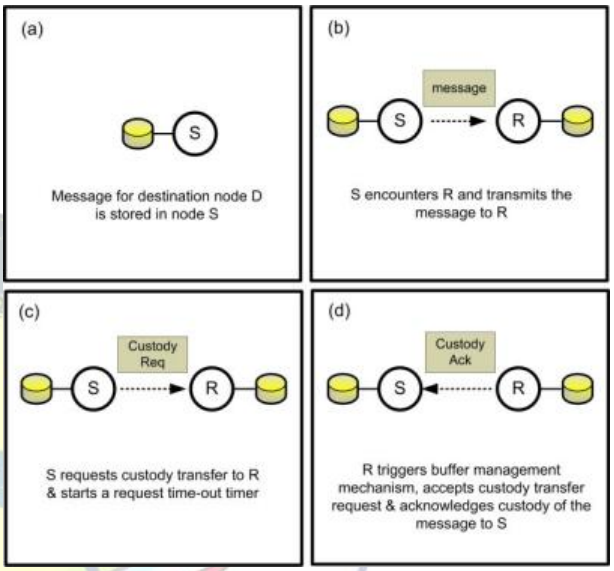

Fig. 4. Interaction of reliability and congestion control strategies in opportunistic networks.

We study the modest custody transfer scenario shown in Fig. 4. A message intended for node D presently resides in the obstinate storage of node S (Fig. 4-a). During its travel, node S meets node R and, based on its routing protocol, regulates that node R is a better communicate of the message to node D. Node S therefore forwards the message to R (Fig. 4-b). S then requests a transfer service for the message to R and starts a request time-out regulator (Fig. 4-c).

Upon receiving the request, R triggers its buffer management device to determine whether receiving the message is likely to lead to buffer congestion in future, and therefore agrees whether to accept or reject the custody request. In the example shown, R accepts the request (Fig. 4-d).

There are two types of congestion in communication networks, namely *link congestion* and *node storage congestion*. A congested link occurs when two or more nodes that are within transmission range cope to transmit message using the same link or channel. However, congested links rarely occur in opportunistic networks. On the other side, congested storage happens when posts compete for the use of partial node storage space. In the remainder of this paper, we will use the term "congestion" to refer to the "storage or buffer congestion" that more regularly occurs in opportunistic networks, given the nodes' partial storage capacity. Congestion control plans in opportunistic networks are closely connected to the number of message duplicates distribute through the network. Routing protocols may use a multiple – copy strategy to increase the delivery ratio and/or to minimize end-to-end delivery latency. In this strategy, several duplicates of a message mingle in the network at any instant. Assumed the presence of redundant messages in the network it is likely that the provision of a custody provision for messages is not needed, and in this case congestion control can be in the form of a *message drop strategy*.

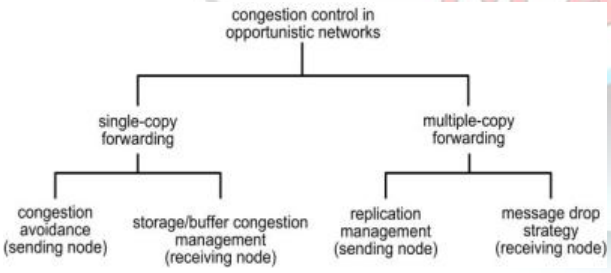

Fig. 5. Congestion control strategies for opportunistic networks

In the fixed Internet, packet dropping is typically completed in the network's relay nodes, i.e. at IP routers. However, when an IP router drops messages during traffic congestion, it does not consider the overall delivery performance in the network. Instead, the end-to-end TCP mechanism guarantees delivery, by requesting the source to retransmit the released messages. In opportunistic networks, as we noted above, the round trip time knows that the end-to- end delivery mechanism is mild temporary and hence dropped messages can't be identified easily by the source.

When an opportunistic network node has to drop messages during congestion, it needs to reflect network delivery performance, for example by dropping those messages that have less impact on the end-to-end delivery. Though, in the case of a single-copy routing strategy, dropping messages during congestion may considerably decrease the overall delivery performance in the network. The congestion control strategy, or *storage congestion management*, should sensibly select which messages are stored in a node so as to avoid forthcoming congestion. As an example, retaining messages that have longer remaining time – to - live (TTLs) is more risky and expensive for node buffer space than storing messages with slight TTLs.

4. CONCLUSION

The opportunistic networks means that certain straight end-to-end transport meanings have to be additionally supported within the network. In particular, transfer reliability and congestion control tools have to be implemented in the network on a per hop basis, and old fixed network roles, such as packet forwarding and dropping and congestion control, become more tightly coupled. In this paper we have provided an summary of the formal of the art of offers for transfer reliability and congestion control in opportunistic networks.

The main focus area of this paper are:

- Considering transfer reliability and congestion control offers attractive explanation of opportunistic networks' features

- Classifying open research issues in reliability and congestion control in opportunistic networks

REFERENCES

[1] T.C.Ezhil Selvan, P.Malathi, S.Ezhilin Freeda, "*Reliable Congestion Control and Link-aware routing protocol (RCLRP) for Mobile Adhoc Networks "*. International Journal of Electronics and Communication Engineering (SSRG-IJECE) Pages 9-17, 2015.

[2] P. Szczytowski, A. Khelil, A. Ali, N. Suri, "TOM: Topology Oriented Maintenance in Sparse Wireless Sensor Networks", *Proc. 8th IEEE SECON*, Salt Lake City, Utah, USA, June 2011.

[3] P. Jacquet, P. Muhlethaler, T. Clausen, A.Laouiti, A. Qayyum, L. Viennot, "Optimized Link State Routing Protocol for Ad Hoc Networks", *Proc. IEEE INMIC*, Lahore, Pakistan, Dec. 2001.

[4] G. Holland, N. Vaidya, "Analysis of TCP Performance over Mobile Ad Hoc Networks", *Proc. ACM MOBICOM*, Seattle, WA, USA, Aug. 1999.

[5] C.Siva Ram Murthy and B. S. Manoj. "*Ad hoc wireless networks: Architecture and Protocols"*. Prentice Hall Publishers, May 2004, ISBN 013147023.

[6] D. Kim, C.K. Toh, Y. Choi, "TCP-BuS: Improving TCP Performance in Wireless Ad Hoc Networks", *J. Communication and Networks*, vol.3, no.2, pp. 1-12, June 2001.

[7] Kimaya Sanzgiri, Bridget Dahill, Brian N. Levine, and Elizabeth M. Belding-Royer. *"A Secure Routing Protocol for Ad Hoc Networks"*. Proceedings of 10th IEEE International Conference on Network Protocols (ICNP'02), Paris, France, November 2002, pp. 78-90.

[8] Y. Hu, A. Perrig, D. Johnson. "*Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks"*. Proceedings of The 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), March 2003.

[9] Yi-an Huang and Wenke Lee. *"Attack analysis and Detection for Ad-hoc Routing protocols"*. Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), French Riviera, France. September 2004.

[10] Hongmei Deng, Wei Li, and Dharma P. Agrawal. "*Routing Security in Wireless Ad Hoc Network*,"**.** IEEE Communications Magazine, vol. 40, no. 10, October 2002.

[11] Space Communication Protocol Standards (SCPS), available online: http://www.scps.org/html/tcp peps.html

[1]**T.C.Ezhil Selvan** received the BE degree in Computer Science and Engineering from Anna University, Chennai, India, in 2006 and the ME degree in Software Engineering from Anna University, Chennai, India, in 2009.He is currently working towards his PhD degree in Information and Communication Technology discipline at Anna University, Chennai, India. His research interest includes Computer Networks, Mobile Computing, Wireless Communication and Network Security.

[2]**Dr.P.Malathi** is working as the Principal at Bharathiyar Institute of Engineering for Women, Salem, India. Her research interest includes Wireless Communication and Digital image processing. She has over 15 years of experience in teaching. Her publications includes 5 National /International journals and 15 National / International Conferences.

[3]**S.Ezhilin Freeda** received the BE degree in Computer Science and Engineering from Anna University, Chennai, India, in 2008 and the ME degree in Computer Science and Engineering from Anna University, Chennai, India, in 2010. His research interests include wireless communications and Data Mining.